UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: **COMMISSIONER FOR PATENTS**
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/009,840	05/01/2002	Olivier Lenoir	USB99 JMC SCU	1234

466 7590 05/31/2006

YOUNG & THOMPSON
745 SOUTH 23RD STREET
2ND FLOOR
ARLINGTON, VA 22202

EXAMINER
BLUDAU, BRANDON S

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/009,840	LENOIR ET AL.
	Examiner	Art Unit	
	Brandon S. Bludau	2132	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _16 March 2006_.

2a) ☐ This action is **FINAL.**   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-12_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-12_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☒ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   This action is in reply to an amendment filed March 16, 2006. Claims 4,8,10 and 11 have been amended. Claims 1-12 are pending.

2.   The Examiner withdraws the previous objection to claims 8 and 10, as the claims have been corrected to over the objection.

3.   The Examiner withdraws the 112 rejection of claim 4, as the claim has been properly amended.

4.   The examiner appreciates the Applicant point out the date discrepancy of Allahwerdi and subsequently withdraws the rejections using this reference. However, new rejections have been made using new art.

Response to Arguments

5.   Applicant's arguments with respect to claims 1-12 in regards to the withdrawn Allahwerdi reference have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

6.   Claim 4 is objected to because of the following informalities: line 6 states "the server authentication data base (BDA) key" in view of the previous amendment, the word "key" should be omitted. Appropriate correction is required.

Claim Rejections - 35 USC § 112

7.   Claim 1 recites the limitation "securing the access" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

8.   .Claims 1-5,7,9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Ratayczak (US Patent 6259909), and further in view of Hodges (US Patent

5420908).

9.   As per claim 1, Ratayczak discloses a process of securing the access to a data

processing server from a client site through at least a first communication network, this

server comprising means for handling a protocol of authenticating a client site user,

comprising a sequence of receiving and processing identification data of a client site

user, and a sequence of transmitting a message from the server site to a client site user

owned communication equipment through a second communication network (column 6

line 59- column 7 line 23), characterized in that this transmitted message is a voice

message (column 7 lines 36-47 wherein using a telephone it is inherent that a voice

message is sent) providing to the aforesaid user means for generating an authentication

password intended to be transmitted to the aforesaid server site through either the first

. or the second communication network, the call number of the aforesaid communication

equipment being searched from an authentication data base (column 4 lines 12-25

wherein the number call number is inherently stored in the subscriber-related data).

Ratayczak does not disclose wherein the process provides to the user means for

generating an authentication password.

Hodges does disclose a process where the data processor provides the user

means for generating an authentication password to be sent back to the processor in

column 3 lines 45-54.

Hodges is analogous art because it is directed to a method of authenticating a user using a mobile telephone device using a challenge response protocol wherein the wireless device uses an encryption key to encrypt a challenge from the authenticator and the authenticator verifies and authenticates the response.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Ratayczak to include providing the user with a means for generating a password such as a key for use in a challenge response protocol.

Motivation for one to modify Ratayczak as discussed above would have been to enhance the security of the authentication method by authorizing a user without having to send the actual password/key across the network as stated in Hodges and as is well known in the art. Challenge-response protocols are very prevalent and widely used in authentication networks to authenticate users. The wide use is attributed to the added security by never having to transmit the secret across the network and preventing replay attacks on an intercepted response.

10. As per claim 2, Ratayczak discloses the securing process according to claim 1, characterized in that it comprises steps of:

Requesting identification data (ID, MPC) from the client site through the first communication network (column 6 lines 59-64);

Processing the aforesaid data (ID, MPC) and searching an authentication database for a client user owned mobile communication equipment call number (this is inherent in column 7 lines 1-5 and 36-44 in that the server must know the call number of the mobile device from the HLR described in column 4 lines 12-24);

Calling the aforesaid communication equipment through at least a second communication network (column 7 lines 1-5 and 36-44);

After establishing a communication with the aforesaid mobile communication equipment, generating a random or pseudo random password (MPA) (column 7 lines 36-40);

Sending a voice message comprising the aforesaid random password through the second communication network (column 7 lines 1-5);

Requesting the user provide, from the client site through the first communication network an authentication password (7 lines 13-15) derived from the aforesaid random or pseudo random password; and

Authenticating the aforesaid authentication password (column 7 lines 13-15).

Ratayczak does not disclose wherein the password from the server is randomly generated or that the authentication password is derived from this random password.

Hodges discloses a method wherein the authenticator generates a challenge that is used to derive the authenticated response. Hodges however does not disclose wherein the challenge is random. However, as is widely known and would be understood by one of ordinary skill in the art, random challenges are extremely common in challenge response protocols and would be an obvious feature in a challenge response authentication method.

Obviousness and motivation to combine Hodges are mentioned in relation to claim 1, as the combination here is similar.

11.   As per claim 3, Ratayczak discloses the process according to claim 2,
characterized in that the authentication password matches the server generated random
or pseudo random password transmitted through the mobile communication equipment
(column 7 lines 1-13).

12.   As per claim 4, Hodges discloses in regards to claim 3, a process characterized
in that the authentication password is built from the random or pseudo random
password generated by the server and transmitted through the mobile communication
equipment, applying a client user known key that is embodied within the server
authentication data base, the authentication step comprising a step of converting the
aforesaid authentication password into a random or pseudo random authentication
password by applying the aforesaid key (column 5 lines 30 –35 wherein the random
challenge is well known and practiced in the art as discussed above).

        Motivation and obviousness are the same as applied to claims 1 and 2 discussed
above.

13.   As per claim 5, Ratayczak discloses the process according to claim 1,
characterized in that the identification data requested from the client consists of a
couple [identification code/client password] (column 6 lines 59-64).

14.   As per claim 7, Ratayczak discloses the securing process according to claim1,
characterized in that it comprises on the server side the steps of:

        Requesting identification data (ID, MPC) from the client site through the first
communication network (column 6 lines 59-64);

Processing the aforesaid data (ID, MPC) and searching an authentication database for a client user owned mobile communication equipment call number (this is inherent in column 7 lines 1-5 and 36-44 in that the server must know the call number of the mobile device from the HLR described in column 4 lines 12-24);

Calling the aforesaid communication equipment through at least a second communication network (column 7 lines 1-5 and 36-44);

In case the communication is established with the aforesaid mobile communication equipment, send a voice message requesting the user to send an encryption key (Column 4 lines 55-62, wherein the codeword can be used as an encryption key as stated in column 7 lines 59-62)

Receiving and recognizing the encryption key transmitted by the client by means of the mobile equipment keyboard (column 4 lines 59-65),

But does not disclose deciphering by means of the aforesaid encryption key an authentication password transmitted by the client through the first communication network, this password resulting from the encryption of a client password performed at the client site by means of the encryption key; and authenticating the client password which results from the authentication password deciphering

Hodges does disclose deciphering by means of the aforesaid encryption key an authentication password transmitted by the client through the first communication network, this password resulting from the encryption of a client password performed at the client site by means of the encryption key; and authenticating the client password which results from the authentication password deciphering (column 5 lines 30-35).

Hodges is analogous art because it is directed to a method for authenticating a user in a challenge response authentication method.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Ratayczak to include using the requested and sent key at the server to encrypt the previously transmitted password/challenge to reveal a subsequent password/response.

Motivation for one to modify Ratayczak as discussed above would have been to enable the transmission of a password without sending the secret data used for the authentication across the network as is discussed in the rejection to claims 1 and 2.

15.   Claim 9 is rejected because it discloses the same subject matter as claim 1.

16.   Claim 10 is rejected because it discloses the same subject matter as claim 2.

17.   Claim 11 is rejected because it discloses the same subject matter as claim 7.

18.   Claim 12 is rejected in regards to claim 1 because it is directed to an application for utilizing the process of claim 1.

19.   Claims 6 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ratayczak (US Patent 6259909), in view of Hodges (US Patent 5420908), and further in view of Fielder (US Patent 5995624)

20.   As per claim 6, Ratayczak and Hodges disclose the process according to claim 1, but do not disclose wherein the process is characterized in that the step of requesting the authentication password from the user takes place during a predetermined time-out delay beyond which authentication is denied.

Fielder does disclose wherein the process is characterized in that the step of requesting the authentication password from the user takes place during a predetermined time-out delay beyond which authentication is denied (column 8 lines 45-49).

Fielder is analogous art because it is directed towards authenticating a user from entry of a password.

It would have been obvious for one of ordinary skill in the art to modify Ratayczak et al. to include a time out interval in which the authentication password needed to be entered.

Motivation for one to modify Ratayczak as discussed above would have been to enhance the security of the process so as to prevent an attack that would use the time delay to intercept the challenge/response or simply to free up processing capability from an authentication session that didn't complete in the necessary time frame. These motivation statements are well known in the art as commonly used in authentication protocols.

21.   As per claim 8, Ratayczak and Hodges disclose the process according to claim 7, but do not disclose wherein it is characterized in that the step of receiving the encryption [key] takes place during a predetermined time-out delay beyond which the authentication is denied.

Fielder does disclose wherein receiving the encryption [key] takes place during a predetermined time-out delay beyond which the authentication is denied (column 8 lines 45-49).

Obviousness and motivation to combine are the same as presented in claim 6 above as it is a similar limitation.
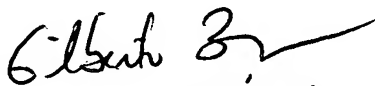
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon S Bludau
Examiner
Art Unit 2132

BB
***

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100